IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

NORMA EGAN and JOSEPH EGAN, individually and on behalf of all others similarly situated, Plaintiffs, v. X-MODE SOCIAL, INC., Defendant.	Civil Action No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Norma Egan and Joseph Egan ("Plaintiffs"), by and through their attorneys, make the following allegations pursuant to the investigation of their counsel and based upon information and belief, except as to allegations specifically pertaining to themselves and their counsel, which are based on personal knowledge, against Defendant X-Mode Social, Inc. ("X-Mode" or "Defendant").

NATURE OF THE ACTION

1. This case challenges X-Mode's unlawful practice of selling highly sensitive personal data of Plaintiffs and Class members after X-Mode purchased the data from third party phone applications.

2. X-Mode violates state law by first acquiring and/or tracking consumers' precise geolocation data and other data and then profiting from that data by selling it to others without obtaining consent. The data can include consumers' movements to and from sensitive locations, like locations associated with medical care, reproductive health, religious worship, mental health, temporary shelters, such as shelters for the homeless, domestic violence survivors, addiction recovery, or other at-risk populations.

3. X-mode purchased geolocation data from third-party phone applications who purportedly obtain consent directly from the mobile device users to collect and share this data. For purposes of this action only, Plaintiffs do not challenge that the specific third-party application who originally obtained their geolocation data obtained their consent to collect and share their data. Any purported consent was on behalf of the specific phone applications and did not apply to Defendant. X-Mode itself, nor any entity acting on its behalf, ever attempted to obtain – or did obtain – consent for its subsequent sale and/or transfer of the data to other third parties after it acquired data from the phone applications.

4. Plaintiffs are individuals who assert claims on behalf of themselves and other similarly situated individuals for unjust enrichment and violations of consumer protection statutes.

5. By selling this data without consent, Defendant has been unjustly enriched and has violated Plaintiffs' privacy rights, state consumer protection and privacy statutes, and Section 5 of the FTC Act.

JURISDICTION AND VENUE

6. Jurisdiction is proper in this Court pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2) because this is a class action in which at least one member of the class is a citizen of a state different from any Defendant, the amount in controversy exceeds $5 million, exclusive of interest and costs, and the proposed class contains more than 100 members.

7. This court has personal jurisdiction over Defendant because Defendant's principal place of business is located in this district.

8. Venue is proper in this district pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to the claims asserted herein occurred in this District and because Defendant's principal place of business is located in this district.

PARTIES

9. Plaintiff Joseph Egan is a resident of Somerville, Massachusetts. In or around January 2021, Plaintiff Joseph Egan downloaded a third-party phone application designed to allow users to know the location of their children or other family members (the "App"). The App tracked the geolocation of Plaintiff Joseph Egan and his family. The App also sold Plaintiff Joseph Egan's location data to Defendant when Plaintiff Joseph Egan used the App. In turn, Defendant sold that data for profit, without obtaining Plaintiff Joseph Egan's consent.

10. Plaintiff Norma Egan is a resident of Somerville, Massachusetts. In or around January 2021, Plaintiff Norma Egan downloaded a third-party phone application designed to allow users to know the location of their children or other family members (the "App"). The App tracked the geolocation of Plaintiff Norma Egan and her family. The App also sold Plaintiff Norma Egan's location data to Defendant when Plaintiff Norma Egan used the App. In turn, Defendant sold that data for profit, without obtaining Plaintiff Norma Egan's consent.

11. Defendant purchased Plaintiffs' and class members' geolocation data from third party phone applications and then sold the location data to other third parties for a profit, without obtaining Plaintiffs' consent to do so.

12. Plaintiffs did not give consent to Defendant to sell their geolocation data to third parties for valuable consideration.

13. Defendant X-Mode Social, Inc. is a Delaware corporation with its principal place of business in Herndon, Virginia. Defendant does not own any property in Massachusetts.

GENERAL BACKGROUND

A. X-Mode Tracks And Identifies Users In "Real Time"

14. X-Mode's business model contains two parts. First, it "collects" mobile application users' geolocation, either by paying apps to integrate their "XDK" spyware or by

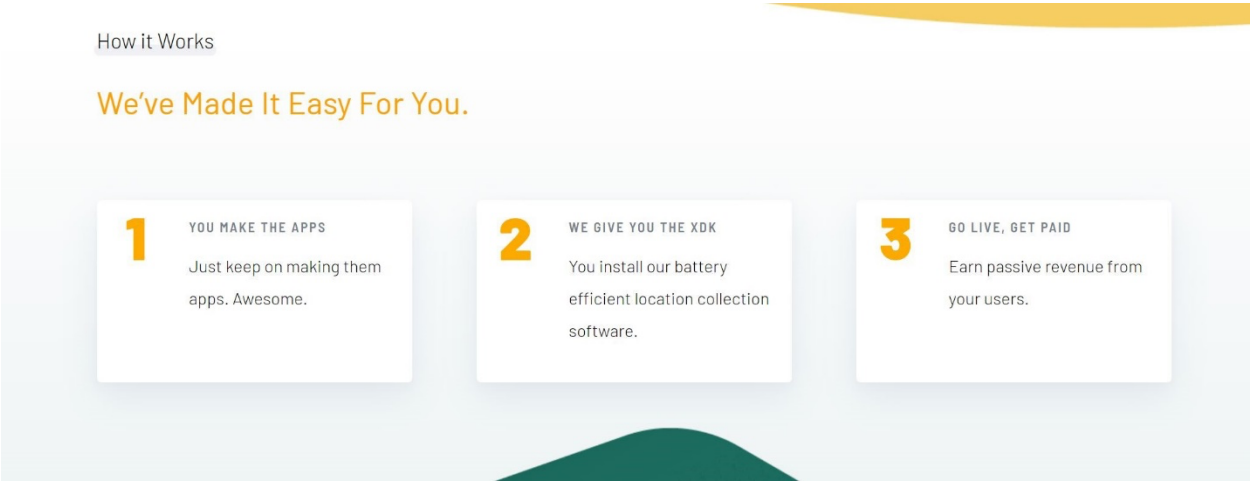
directly paying apps to make server-to-server transfers of collected user geolocation data. Then, on the other side of its business model, Defendant sells this this data to whoever wants it.

15. The geolocation data can be collected through a "Software Development Kit" or "SDK" that X-Mode created. An SDK is piece of software code that any mobile application available on iOS or Android app stores can integrate with their software.

16. X-Mode pays mobile application developers to integrate X-Mode's SDK, aptly named "XDK," into their apps.

17. XDK's function is to collect the location data of all mobile application users which have XDK spyware embedded.

18. For example, X-Mode advertised XDK as an "easy" way for app owners to earn revenue. "1. You make the apps. Just keep on making them [sic] apps. Awesome. 2. We give you the XDK. You install our battery efficient location collection software. 3. Go live, get paid. Earn passive revenue from your users."



19. Once the XDK spyware is on a mobile application, X-Mode receives the data whenever a user runs the application.

20. Even if an individual were aware of the spyware, they would have no ability to disable the transmissions.

21. X-Mode in fact touts that with their data they can send ads "in near-real time of folks who have walked by [a] kiosk or billboard to retarget them online based on when they walked by the kiosk."

22. The tracking SDK spyware always transmits the IP address of the user, which is used to derive location information for purposes of analytics and reporting.

23. X-Mode stated, in recent court filings, that it collects and sells the "precise latitude and longitude coordinates" of XDK-enabled mobile application users in "raw form," i.e., geolocation correlated directly to the mobile application users' personal identifiers. X-Mode also touts that the XDK spyware is imbedded in over four hundred apps.

24. Thus, using its spyware, X-Mode monitors, tracks, and identifies consumers in "real time."

25. Alternatively, X-Mode also pays applications to obtain already collected geolocation data from the apps through direct server-to-serve transfers. X-mode then uses the data is directly purchased to monitor, track, and identify consumers.

B. X-Mode Sells Precise Location Information for Hundreds of Millions of Mobile Devices

26. X-Mode is primarily a location data broker that provides its customers massive amounts of precise geolocation data collected from consumers' mobile devices. Through X-Mode's services customers can license location data including "near real-time" and "historical location data" of a consumer's mobile device, and a timestamp of when a person was at the location.

27. In or about June 2019, X-Mode declared that they were "committed to making our data available to as many people as possible," and began to offer their sensitive location data to the public on Amazon Web Services ("AWS") Marketplace.

28. Any person can buy X-Mode's "high quality, SDK-sourced location data" on the AWS Marketplace.

29. X-Mode's "scale" of data include "60M+ global MAU (Monthly Active Users), 400+ mobile app publishers with our XDK, [and] 25% of the adult U.S. population monthly."

30. This data is used by clients for measuring ad campaign "effectiveness." For example, "X-Mode gives you that ability to validate if the customer visited your store within hours or days after seeing your ad online" with "near real-time attribution."

31. The data can also be used for targeting campaigns. For example, if "[a client] wants to target folks who have just bought a new phone because they sell an affordable low cost warranty program. They use X-Mode's data to target 1M+ users a month whom have been in a Best Buy, Apple Store, and T-Mobile in the past 48 hours."

32. More alarmingly, "X-Mode can send data in near-real time of folks who have walked by their kiosk or billboard to retarget them online based on when they walked by the kiosk" by matching "the timestamp of when the ad was shown to the timestamp of when the device ID was near the kiosk."

33. The "device ID" X-Mode uses to match location with is also known as a Mobile Advertising ID ("MAID").

34. A MAID is a unique identifier assigned to a consumer's mobile device to assist marketers in advertising to the consumer.

35. X-Mode thus sells the geolocation correlated to the MAIDs of "25%+ of the Adult U.S. population monthly" (including Plaintiffs and other putative class members) which

includes Wi-Fi data, cell tower triangulation, dwell times near points of interest, MAIDs, time and date information, device type, operating system version and type, device settings, device time zone, device carrier, and current IP address.

36. X-Mode has also faced controversy over how it handles data and privacy. X-Mode was banned from most app stores after it was discovered that the company was selling location data from Muslim prayer apps like Muslim Pro to U.S. government contractors associated with national security, raising concerns about unconstitutional government surveillance. Public records show that Defendant received at least $423,000 from the U.S. Air Force and the Defense Intelligence Agency for location data. Defendant also sold data on Americans in profiled sets, like people who were drivers or likely to shop at department stores.

C. X-Mode's Data Can Be Used to Identify People and Track Them to Sensitive Locations

37. Precise geolocation data associated with MAIDs, such as the data sold by X-Mode, may be used to track consumers to sensitive locations, including places of religious worship, places that may be used to infer an LGBTQ+ identification, domestic abuse shelters, medical facilities, and welfare and homeless shelters.

38. By plotting the latitude and longitude coordinates provided by X-Mode with publicly available map programs, it is possible to identify which consumers' mobile devices visited reproductive health clinics. Further, because each set of coordinates is time-stamped, it is also possible to identify when a mobile device visited the location. Similar methods may be used to trace consumers' visits to other sensitive locations.

39. The location data provided by X-Mode is not anonymized, or alternatively, is easily de-anonymized. It is possible to use the geolocation data, combined with the mobile device's MAID, to identify the mobile device's user or owner. For example, some data brokers

advertise services to match MAIDs with "offline" information, such as consumers' names and physical addresses.

40. Location data can be easily used to identify people. The location data sold by X-Mode typically includes multiple timestamped signals for each MAID.

41. By plotting each of these signals on a map, much can be inferred about the mobile device owners. For example, the location of a mobile device at night likely corresponds to the consumer's home address. Public or other records may identify the name of the owner or resident of a particular address.

42. X-Mode employs no technical controls to prohibit its customers from identifying consumers or tracking them to sensitive locations. For example, it does not employ a blacklist that removes from its data set location signals around sensitive locations including, among others, locations associated with medical care, reproductive health, religious worship, mental health, temporary shelters, such as shelters for the homeless, domestic violence survivors, or other at-risk populations, and addiction recovery. In fact, X-Mode recently resorted to suing a former client that resold their raw geolocation data because it does not have any technical way to restrict what their clients do with the data.

D. Defendant's Practices Cause and Are Likely to Cause Substantial Injury to Consumers

43. As described above, the data sold by Defendant may be used to identify individual consumers and their visits to sensitive locations. The sale of such data poses an unwarranted intrusion into the most private areas of consumers' lives and causes or is likely to cause substantial injury to consumers.

44. For example, the data may be used to identify consumers who have visited an abortion clinic and, as a result, may have had or contemplated having an abortion.

45. In fact, it is possible to identify a mobile device that visited a women's reproductive

health clinic and trace that mobile device to a single-family residence. The data set also reveals that the same mobile device was at a particular location at least three evenings in the same week, suggesting the mobile device user's routine. The data may also be used to identify medical professionals who perform, or assist in the performance, of abortion services.

46. As another example, the data could be used to track consumers to places of worship, and thus reveal the religious beliefs and practices of consumers.

47. As another example, the data could be used to track consumers who visited a homeless shelter, domestic violence shelter, or other facilities directed to at-risk populations. This information could reveal the location of consumers who are escaping domestic violence or other crimes.

48. In addition, because Defendant's data allows its customers to track consumers over time, the data could be used to identify consumers' past conditions, such as homelessness.

49. As another example, the data could be used to track consumers who have visited addiction recovery centers. The data could show how long consumers stayed at the center and whether a consumer relapses and returns to a recovery center.

50. Identification of sensitive and private characteristics of consumers from the location data sold and offered by Defendant injures or is likely to injure consumers through exposure to stigma, discrimination, physical violence, emotional distress, and other harms.

51. These injuries are exacerbated by the fact that once Defendant sells the data, it lacks any meaningful controls over who accesses its location data feed.

52. The collection and use of consumer location data are opaque to consumers, who typically do not know who has purchased their location data or how it is being used. Indeed, once information is collected about consumers from their mobile devices, the information can be sold multiple times to companies that consumers have never heard of and never interacted with.

Consumers have no insight into how this data is used – they do not, for example, typically know or understand that the information collected about them can be used to track and map their past movements and that inferences about them and their behaviors will be drawn from this information. Consumers are therefore unable to take reasonable steps to avoid the above-described injuries.

53. The harms described above are not outweighed by countervailing benefits to consumers or competition.

54. For these reasons, the Federal Trade Commission ("FTC") took action against Defendant in January 2024 to restrain Defendant from engaging in the above conduct. *See In the Matter of X-Mode Social, Inc.*, FTC Matter/File Number 2123038.

55. According to the FTC, the "Unfair Sale of Sensitive Data," as described above constitutes a violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which prohibits "unfair or deceptive acts or practices in or affecting commerce."

56. Acts or practices are unfair under Section 5 of the FTC Act if they cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n).

CLASS REPRESENTATION ALLEGATIONS

57. Plaintiffs seek to represent a class defined as all persons in the United States whose data, including but not limited to their geolocation data, was sold by Defendant without their consent (the "Class").

58. Plaintiffs also seek to represent a subclass defined as all Class members who reside in the Commonwealth of Massachusetts whose data, including but not limited to their geolocation data, was sold by Defendant without their consent (the "Massachusetts Subclass").

59. Subject to additional information obtained through discovery, the foregoing class definitions may be modified or narrowed by an amended complaint, or at class certification, including through the use of multi-state subclasses to account for material differences in state law, if any.

60. Members of the Class and Massachusetts Subclass are so numerous that their individual joinder herein is impracticable. On information and belief, members of the Class and Massachusetts Subclass number in the millions. The precise number of Class members and their identities are unknown to Plaintiffs at this time but may be determined through discovery. Class members may be notified of the pendency of this action by mail and/or publication through the distribution records of Defendant and third-party retailers and vendors.

61. Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Common legal and factual questions include but are not limited to whether Defendant's sale of geolocation data without consent constitutes unjust enrichment.

62. The claims of the named Plaintiffs are typical of the claims of the Class in that the named Plaintiffs' data was sold by Defendant without their consent, and the named Plaintiffs suffered injury as a result of Defendant's conduct.

63. Plaintiffs are adequate representatives of the Class and Massachusetts Subclass because their interests do not conflict with the interests of the Class members they seek to represent, they have retained competent counsel experienced in prosecuting class actions, and they intend to prosecute this action vigorously. The interests of Class members will be fairly and adequately protected by Plaintiffs and their counsel.

64. The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of Class members. Each individual Class member may lack the

resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by the complex legal and factual issues of this case. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

COUNT I

Unjust Enrichment

65. Plaintiffs incorporate by reference and re-allege each and every allegation set forth above as though fully set forth herein.

66. Plaintiffs bring this claim individually and on behalf of members of the Class and the Massachusetts Subclass against Defendant.

67. Plaintiffs and Class members unwittingly conferred a benefit upon Defendant. Defendant acquired valuable personal location information belonging to Plaintiffs and Class members which it then sold to other parties without the consent of Plaintiffs and Class members. Plaintiffs and Class members received nothing from this transaction. Plaintiffs lack an adequate remedy at law, and pleads this cause of action in the alternative to the extent Plaintiffs are required to do so.

68. Defendant has knowledge of such benefits.

69. Defendant has been unjustly enriched in retaining the revenues derived from the sale of Plaintiffs' and Class members' data, including their geolocation data. Retention of those moneys under these circumstances is unjust and inequitable because Defendant did not obtain the

consent of Plaintiffs and Class members before selling their data to third parties as described above.

70. Because Defendant's retention of the non-gratuitous benefits conferred on it by Plaintiffs and Class members is unjust and inequitable, Defendant must pay restitution to Plaintiffs and the Class members for its unjust enrichment, as ordered by the Court.

COUNT II
Violation of the Massachusetts Unfair and Deceptive Business Practices Act, Mass. Gen. Laws Ch. 93A *et seq.*

71. Plaintiffs incorporate by reference and re-allege each and every allegation set forth above as though fully set forth herein.

72. Plaintiffs bring this claim individually and on behalf of the members of the Massachusetts Subclass against Defendant.

73. Section 2 of Chapter 93—the Massachusetts Unfair and Deceptive Business Practices Act ("93A")—prevents the use of "unfair or deceptive acts or practices in the conduct of any trade or commerce."

74. It is "the intent of the legislature that in construing" whether an act is deceptive under 93A § 2, "the courts will be guided by the interpretations given by the Federal Trade Commission and the Federal Courts to section 5(a)(1) of the Federal Trade Commission Act (15 U.S.C. 45(a)(1)), as from time to time amended." *See* Mass. Gen. Laws Ann. Ch. 93A, § 2.

75. An act or practice is a violation of 93A if it "violates the Federal Trade Commission Act, the Federal Consumer Credit Protection Act or other Federal consumer protection statutes within the purview of M.G.L. Ch. 93A, § 2." 940 CMR 3.16.

76. Section 9 provides: "Any person … who has been injured by another person's use or employment of any method, act or practice declared to be unlawful by section two … may bring an action in the superior court … for damages and such equitable relief, including an

injunction, as the court deems to be necessary and proper … Any persons entitled to bring such action may, if the use or employment of the unfair or deceptive act or practice has caused similar injury to numerous other persons similarly situated and if the court finds in a preliminary hearing that he adequately and fairly represents such other persons, bring the action on behalf of herself and such other similarly injured and situated persons."

77. Pursuant to the definitions codified in Chapter 93A § 1, Defendant is a "person," and Defendant is engaged in "trade" and "commerce" in Massachusetts by engaging in the purchase and sale of Products that directly or indirectly affect the people of Massachusetts.

78. By engaging in the acts and omissions alleged above and incorporated herein, Defendant has engaged and continues to engage in unfair or deceptive acts or practices in the conduct of trade or commerce.

79. Defendant's misrepresentations deceive and have a tendency to deceive a reasonable consumer and the general public.

80. Defendant's acts and omissions are material, in that a reasonable person would attach importance to the information and omissions described above and would be induced to act on the information in deciding to use services such as phone applications.

81. Defendant has also committed a violation of 93A predicated on its violations of FTC regulations – specifically, its violation of Section 5 of the FTC Act as interpreted by the Federal Trade Commission.

82. Plaintiffs and members of the Massachusetts Subclass were deceived by Defendant's policies and in fact had no idea that Defendant was selling their location data.

83. Plaintiffs and members of the Massachusetts Subclass did not consent to Defendant's sale of their location data.

84. Defendant in conjunction with third party phone and internet applications knowingly omitted that Defendant had access to and was selling the location data of Plaintiffs and the class.

85. Had Plaintiffs and Massachusetts Subclass members known that the Defendant was selling their data, they would have requested compensation for the misappropriation and sale of their location data.

86. Plaintiffs and Massachusetts Subclass Members were injured as a direct and proximate result of Defendant's breach because Defendant misappropriated and sold the location data of Plaintiffs and Massachusetts Subclass members without consent.

87. Plaintiffs and members of the Massachusetts Subclass have been harmed by this injury, adverse consequence, and/or loss.

88. 93A represents a fundamental public policy of the Commonwealth of Massachusetts.

89. For each loss, Plaintiffs and each member of the Massachusetts Subclass may recover an award of actual damages or twenty-five dollars, whichever is greater. Ch. 93A § 9(3).

90. Disgorgement of profit derived from an unfair and deceptive act or practice is a permissible damage remedy under M.G.L. Ch. 93A, § 9.

91. Accordingly, Plaintiffs and the members of the Massachusetts Subclass seek the disgorgement of profits that Defendant derived from the sale of their location data.

92. Because Defendant acted willfully or knowingly, Plaintiffs and each member of the Massachusetts Subclass may recover up to three but not less than two times this amount. In addition, Plaintiffs may recover attorneys' fees and costs.

93. Plaintiffs and each member of the Massachusetts Subclass may recover an award of actual damages (in this case unlawful profit derived from the sale and trading of location data)

or twenty-five dollars, whichever is greater. Ch. 93A § 9(3).

94. Plaintiffs and the members of the Massachusetts Subclass may also seek the imposition of an injunction relief which limits and polices Defendant's representations within or reaching Massachusetts. The balance of the equities favors the entry of permanent injunctive relief against Defendant. Plaintiffs, members of the Massachusetts Subclass, and the general public will be irreparably harmed absent the entry of permanent injunctive relief against Defendant. Plaintiffs, members of the Massachusetts Subclass, and the general public lack an adequate remedy at law. A permanent injunction against Defendant is in the public interest. Defendant's unlawful behavior is capable of repetition or re-occurrence absent the entry of a permanent injunction.

RELIEF DEMANDED

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

a. For an order certifying the nationwide Class and the Massachusetts Subclass under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiffs as representatives of the Class and the Massachusetts Subclass and Plaintiffs' attorneys as Class Counsel to represent the Class and the Massachusetts Subclass members;

b. For an order declaring that Defendant's conduct violates the laws referenced herein;

c. For an order finding in favor of Plaintiffs, the nationwide Class, and the Massachusetts Subclass on all counts asserted herein;

d. For compensatory, statutory, and punitive damages in amounts to be determined by the Court and/or jury;

e. For prejudgment interest on all amounts awarded;

f. For an order of restitution and all other forms of equitable monetary relief;

g. For an order enjoining Defendant from continuing the illegal practices detailed herein and compelling Defendant to undertake a corrective advertising campaign; and

h. For an order awarding Plaintiffs and the Class and Massachusetts Subclass their reasonable attorneys' fees and expenses and costs of suit.

JURY TRIAL DEMANDED

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury on all claims so triable.

Dated: June 15, 2023

Respectfully submitted,

BURSOR & FISHER, P.A.

By: */s/*
Joshua Erlich, VSB No. 81298
The Erlich Law Office, PLLC
1550 Wilson Blvd., Ste. 700
Arlington, VA 22209
Phone: 703-791-9087
Fax: 703-722-8114
jerlich@erlichlawoffice.com

BURSOR & FISHER, P.A.
Joseph I. Marchese (*pro hac vice* forthcoming)
Julian C. Diamond (*pro hac vice* forthcoming)
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Tel: (646) 837-7150
Fax: (212) 989-9163
E-Mail: jmarchese@bursor.com
jdiamond@bursor.com

Attorneys for Plaintiffs